

G-03

System Certyfikacji PL Portfela EUDI

Organizacja i wsparcie właściciela
krajowego systemu certyfikacji EUDI

WERSJA 1.01

2026.07.20

Oznaczenie dokumentu	G-03
Wersja	1.01
Status	Final
Data	20.07.2026
Rodzaj dokumentu	Dokument ramowy
Ramy nadrzędne	brak
Właściciel programu	Rzeczpospolita Polska / Minister Cyfryzacji
Przedmiot certyfikacji	System Certyfikacji PL Portfela EUDI
Odbiorcy pierwotni	Właściciel systemu, organ nadzoru
Odbiorcy wtórni	Jednostki CAB, dostawcy PID, dostawcy portfela
Poziom uzasadnienia zaufania <potwierdzenie tożsamości, CIR 2015/1502> lub <ocena, rozporządzenie (UE) 2019/881>	Wysoki/Wysoki
Dokumenty podrzędne	GP-01, GP-02, GP-03

Historia zmian

Lp.	Zmiana	Wersja	Data
1.	Wersja oficjalna	1.0	2026-06-25
2.	Poprawki redakcyjne	1.01	2026-07-20

Spis treści

1	ZAKRES	6
2	DOKUMENTY PRAWNE I NORMATYWNE.....	7
3	ŁAD ORGANIZACYJNY I ZARZĄDZANIE PROGRAMEM.....	9
3.1	Rozwiązania organizacyjne Ministerstwa Cyfryzacji	9
3.2	Procesy utrzymania i procedury przeglądu po stronie Właściciela programu.....	9
3.3	Wzajemna ocena (peer review).....	10
3.3.1	Ocena wstępna prowadzona przez Grupę Współpracy na rzecz Europejskiej Tożsamości Cyfrowej	10
3.3.2	Regularna wzajemna ocena.....	10
4	ZARZĄDZANIE PODATNOŚCIAMI TECHNICZNYMI.....	13
4.1	Zarządzanie podatnościami technicznymi: wsparcie obsługi podatności technicznych	13
5	ZNAKI I OZNACZENIA	15
5.1	Znak zaufania Portfela EUDI	15
5.2	Znak zgodności w ramach Systemu Certyfikacji PL Portfela EUDI	16
5.3	Projekt i formaty.....	17
5.4	Zasady używania znaku zgodności.....	17
6	RAMY ZAUFANIA (TRUST FRAMEWORK)	19
6.1	Ramy regulacyjne nadzoru nad europejskim portfelem tożsamości cyfrowej	19
6.2	Ramy zaufania: ustanowienie i utrzymanie pod egidą organu nadzoru.....	20
6.3	Zgodność dostawców portfela z ramami zaufania	21
6.4	Sprawozdawczość dotycząca ekosystemu Portfela EUDI	22
6.4.1	Postanowienia ogólne	22
6.4.2	Procedury notyfikowania Komisji Europejskiej ekosystemu Portfela EUDI.....	23
7	SZCZEGÓLNE PROCEDURY NOTYFIKACJI I SPRAWOZDAWCZOŚCI W ODNIESIENIU DO SYSTEMU CERTYFIKACJI.....	25
7.1	Zmiany statusu certyfikatu.....	25
7.1.1	Notyfikacja wyników: procedury notyfikowania wyników certyfikacji i działań nadzoru Właścicielowi systemu/programu	25
7.1.2	Notyfikacja Komisji Europejskiej i EUDICG.....	25
7.2	Notyfikacja w NANDO.....	26
7.2.1	Pierwsza notyfikacja polskich CAB w NANDO.....	26
7.2.2	Aktualizacje wpisów w NANDO.....	27
8	ROZPATRYWANIE SKARG	29
9	PROCEDURY TECHNICZNE WŁAŚCICIELA SYSTEMU	31

9.1	Ochrona informacji.....	31
9.2	Bezpieczna wymiana informacji	31
9.2.1	Najnowocześniejsze mechanizmy kryptograficzne zatwierdzone przez Właściciela systemu	31
9.2.2	Lista stosowanych mechanizmów i aplikacji dla CAB-CB, CAB-ITSEF i wnioskodawców	31

1 Zakres

- 1 W niniejszym dokumencie wskazano obowiązki i procedury Właściciela systemu w odniesieniu do systemu certyfikacji Portfela EUDI ustanowionego i wdrożonego w Rzeczypospolitej Polskiej. Dodatkowo opisano rolę organu nadzoru w dozorowaniu ram zaufania (Trust Framework) ze względu na jej istotny wpływ na ryzyka dotyczące usług związanych z Portfelem EUDI, które podlegają certyfikacji.
- 2 Obecnie poza zakresem niniejszego dokumentu pozostają obowiązki nadzorcze wobec wszystkich interesariuszy ekosystemu Portfela EUDI z wyjątkiem dostawców portfela i dostawców PID.
- 3 *UWAGA 1: W kontekście systemu certyfikacji PL Portfela EUDI role Właściciela systemu (System Owner) i Właściciela programu (Scheme Owner) są synonimami.*
- 4 *UWAGA 2: W kontekście ekosystemu Portfela EUDI zastosowanie ma rola organu nadzoru (Supervisory Authority).*
- 5 Język normatywny
- 6 Wymagania oznaczono czasownikiem „musi” („shall”). Stwierdzenia faktów wyrażono prostymi zdaniami oznajmującymi. Wszelkie wskazówki lub wyjaśnienia przedstawiono w formie UWAG i oznaczono kursywą.

2 Dokumenty prawne i normatywne

- 7 W celu prowadzenia certyfikacji europejskich portfeli tożsamości cyfrowej ustanawia się system certyfikacji w zakresie zgodności z rozporządzeniem (UE) 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej, oparty na normach PN-EN ISO/IEC 17067 i PN-EN ISO/IEC 17065 oraz działający w ramach systemu akredytacji opisanego w rozporządzeniu (UE) 765/2008.
- 8 System certyfikacji Portfela EUDI i jego programy wykazują zgodność z następującymi aktami prawnymi:
- I. Ramy funkcjonalne rozporządzenia (UE) 910/2014 (art. 5a) oraz odpowiednie rozporządzenia wykonawcze Komisji:
 - o EU 2024/2977
 - o EU 2024/2979
 - o EU 2024/2980
 - o EU 2024/2982
 - II. Zasady certyfikacji (art. 5c, art. 45a ust. 4 rozporządzenia (UE) 910/2014) oraz rozporządzenie wykonawcze Komisji (UE) 2024/2981
 - III. Europejski program certyfikacji cyberbezpieczeństwa EUCC określony w rozporządzeniu wykonawczym Komisji (UE) 2024/482
 - IV. Art. 58–59 rozporządzenia (UE) 2019/881 (Akt o Cyberbezpieczeństwie)
 - V. Art. 8 ust. 3 rozporządzenia UE 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych wraz z rozporządzeniem wykonawczym Komisji (UE) 2015/1502
 - VI. Częściowe zastosowanie rozporządzenia wykonawczego Komisji 2025/1568 ustanawiającego zasady stosowania rozporządzenia (UE) 910/2014 w odniesieniu do uzgodnień proceduralnych dotyczących wzajemnych ocen systemów identyfikacji elektronicznej oraz współpracy przy organizacji takich ocen w ramach Grupy ds. Współpracy, a także uchylającego decyzję wykonawczą Komisji (UE) 2015/296 — w zakresie wzajemnych ocen krajowego systemu/programów certyfikacji Portfela EUDI
 - VII. Ustawa z 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej

- VIII. Ustawa z 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa
- IX. ETSI TS 119 612 — V2.3.1 — Electronic Signatures and Trust Infrastructures (ESI); Trusted Lists (Zaufane listy)

3 Ład organizacyjny i zarządzanie programem

3.1 Rozwiązania organizacyjne Ministerstwa Cyfryzacji

- 9 Rola Właściciela systemu/programu jest przypisana właściwej komórce w Ministerstwie Cyfryzacji odpowiedzialnej za rozwój ekosystemu cyfrowej tożsamości zgodnie z postanowieniami polskiego aktu prawnego wydanego przez Ministra Cyfryzacji.

3.2 Procesy utrzymania i procedury przeglądu po stronie Właściciela programu

- 10 Właściciel programu musi zapewnić ciągłą zgodność systemu certyfikacji PL Portfela EUDI z wymaganiami ustanowionymi na mocy rozporządzenia (UE) 910/2014, powiązanych rozporządzeń wykonawczych Komisji oraz (opcjonalnie) Ram Architektury i Odniesienia (ARF).
- 11 Właściciel programu musi utrzymywać program poprzez ustanowienie i wdrożenie bieżącego monitorowania zmian w ekosystemie europejskiego portfela tożsamości cyfrowej, takich jak zmiany przepisów, specyfikacji technicznych i wymagań interoperacyjności.
- 12 W przypadku zmian unijnych ram regulacyjnych lub technicznych albo jakiegokolwiek innej istotnej zmiany dotyczącej programu Właściciel programu musi ocenić ich znaczenie oraz — w razie potrzeby — zaktualizować rozwiązania w zakresie ładu organizacyjnego, dokumentację programu i procedury operacyjne, aby utrzymać pełną spójność z obowiązującymi wymaganiami.
- 13 Aby utrzymać zgodność systemu certyfikacji PL Portfela EUDI, Właściciel programu musi integrować informacje pochodzące z certyfikacji, notyfikacji, wzajemnych ocen, działań monitorujących oraz sprawozdawczości statystycznej w celu zapewnienia ciągłego bezpieczeństwa, zaufania i interoperacyjności programu.
- 14 Niezależnie od przeglądów uruchamianych ad hoc w wyniku istotnych zmian technicznych lub regulacyjnych, Właściciel programu musi ustanowić, wdrożyć i stosować procedurę przeglądu prowadzonego okresowo, gwarantując w ten sposób trwałą zgodność w całym cyklu życia operacyjnego programu.
- 15 W zakresie zmian programu wynikających z incydentów bezpieczeństwa lub obsługi podatności — zob. rozdział 4.

3.3 Wzajemna ocena (peer review)

3.3.1 Ocena wstępna prowadzona przez Grupę Współpracy na rzecz Europejskiej Tożsamości Cyfrowej

16 Zgodnie z art. 5c ust. 4 rozporządzenia (UE) 910/2014 Właściciel systemu musi przekazać projekty krajowych programów certyfikacji Europejskiej Grupie Współpracy na rzecz Europejskiej Tożsamości Cyfrowej.

17 *UWAGA 1: Grupa Współpracy na rzecz Europejskiej Tożsamości Cyfrowej może wydawać opinie i zalecenia.*

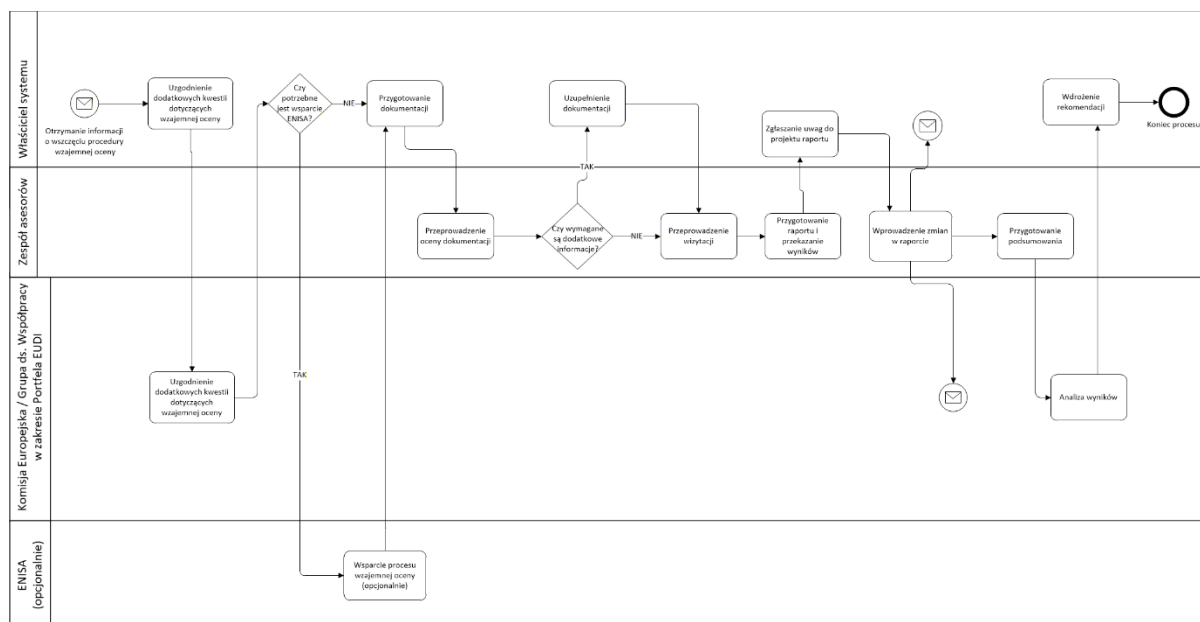
3.3.2 Regularna wzajemna ocena

18 *UWAGA 1: Państwa członkowskie mogą wdrożyć rozwiązanie umożliwiające poddawanie krajowych systemów/programów certyfikacji Portfela EUDI wzajemnej ocenie.*

19 *UWAGA 2: Wobec braku szczegółowych regulacji UE dotyczących wzajemnych ocen systemów/programów certyfikacji proponuje się przyjęcie rozwiązań tymczasowych opartych na rozporządzeniu wykonawczym Komisji (UE) 2025/1568.*

20 *UWAGA 3: Dodatkowo proponowana procedura opiera się na wzajemnej ocenie NCCA określonej w rozporządzeniu wykonawczym Komisji (UE) 2024/482.*

21 *UWAGA 4: Procedura wzajemnej oceny ma na celu ocenę skuteczności, spójności i zgodności działań realizowanych przez właścicieli systemów, którzy za nie odpowiadają. Zapewnia ona ustrukturyzowany mechanizm oceny procesów certyfikacji i nadzoru, identyfikowania obszarów wymagających poprawy oraz wspierania zharmonizowanego wdrażania wymagań certyfikacji Portfela EUDI we wszystkich państwach członkowskich. Proces wzajemnej oceny przedstawiono na Rysunek 1.*



Rysunek 1 Procedura wzajemnej oceny właścicieli systemów

UWAGA 5: Ponieważ wzajemna ocena może być przeprowadzana wyłącznie na zasadzie dobrowolności, poniższy opis nie zawiera żadnych wymagań.

Proces wzajemnej oceny jest realizowany w ścisłej współpracy pomiędzy właścicielami systemów, Komisją Europejską, Zespołem Asesorów oraz — w razie potrzeby — Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Na wstępie ustalane są kwestie organizacyjne, w tym harmonogram oceny, zakres przeglądu oraz inne sprawy proceduralne niezbędne do przeprowadzenia ewaluacji.

Centralnym elementem procedury jest przygotowanie i przekazanie dokumentacji dotyczącej działań certyfikacyjnych i nadzorczych realizowanych przez Właściciela systemu. Dokumentacja podlega szczegółowej ocenie przez Zespół Asesorów, który ocenia zgodność procesów, procedur i mechanizmów nadzorczych z obowiązującymi wymaganiami. W trakcie przeglądu asesory mogą identyfikować luki, niespójności lub obszary wymagające wyjaśnienia, co skutkuje wnioskami o dodatkowe informacje i dokumentację uzupełniającą.

Oprócz przeglądu dokumentacji może być przeprowadzona wizytacja, z uwzględnieniem zasad bezpieczeństwa i ruchu osobowego obowiązującego w siedzibie właściciela programu. Celem wizytacji jest weryfikacja praktycznego wdrożenia procesów certyfikacji i nadzoru, ocena skuteczności rozwiązań organizacyjnych oraz potwierdzenie, że udokumentowane procedury są konsekwentnie stosowane w praktyce.

Wizytacja może obejmować wywiady z personelem, badanie wybranych przypadków oraz weryfikację działań operacyjnych.

- 27 Wynikiem oceny jest raport z wzajemnej oceny zawierający ustalenia z ewaluacji, w tym zidentyfikowane mocne strony, obszary wymagające poprawy, niezgodności oraz zalecenia. Przed sfinalizowaniem raportu Właściciel programu ma możliwość zapoznania się z wersją roboczą i zgłoszenia uwag. Zespół Asesorów rozpatruje zgłoszone uwagi i — w uzasadnionych przypadkach — wprowadza poprawki do raportu końcowego. W przypadku istotnych rozbieżności do raportu może zostać dołączony protokół rozbieżności jako załącznik, aby zapewnić przejrzystość i obiektywność wyników oceny.
- 28 Po zakończeniu przeglądu może zostać przygotowane i udostępnione publicznie podsumowanie procesu wzajemnej oceny. Raport końcowy jest przekazywany Grupie ds. Współpracy na rzecz Portfela EUDI, która analizuje wyniki i może wydać dodatkowe zalecenia lub wytyczne mające na celu poprawę skuteczności i spójności działań certyfikacyjnych w dziedzinie cyberbezpieczeństwa w Unii Europejskiej.
- 29 Ostatnim etapem procedury jest wdrożenie zaleceń wynikających z wzajemnej oceny. Właściciel systemu odpowiada za koordynację działań doskonalących, monitorowanie ich wdrażania oraz zapewnienie usunięcia zidentyfikowanych niedociągnięć. W konsekwencji mechanizm wzajemnej oceny służy nie tylko jako instrument oceny, lecz także jako narzędzie wspierające ciągłe doskonalenie, wzajemne uczenie się oraz harmonizację praktyk certyfikacyjnych związanych z Portfelem EUDI we wszystkich państwach członkowskich.

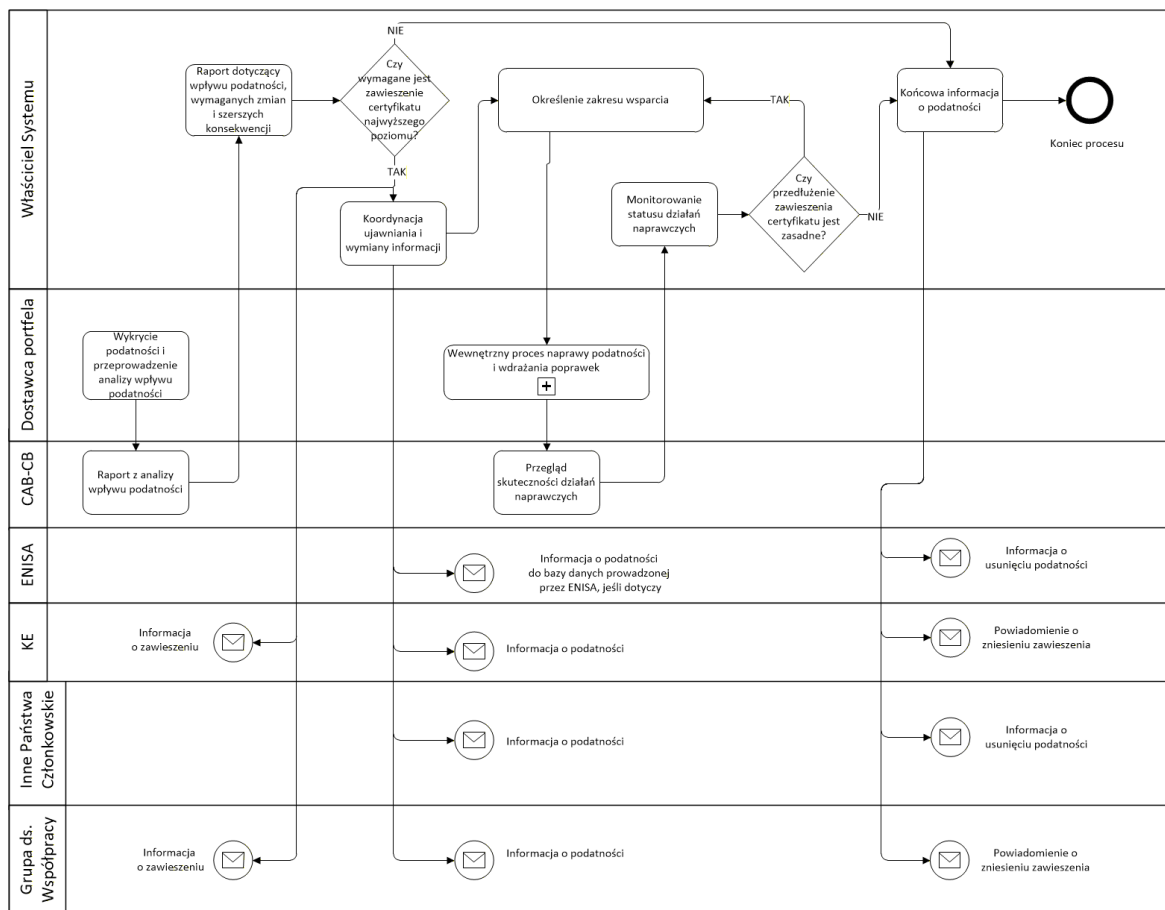
4 Zarządzanie podatnościami technicznymi

4.1 Zarządzanie podatnościami technicznymi: wsparcie obsługi podatności technicznych

30 *UWAGA 1: Niniejsza procedura wysokiego poziomu odnosi się do programów certyfikacji GP-02 i GP-03.*

31 *UWAGA 2: Zarządzanie podatnościami technicznymi jest krytycznym elementem ram bezpieczeństwa operacyjnego programu Portfela EUDI. Zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2981 oraz wymaganiami dyrektywy NIS 2 proces ten ustanawia formalne, skoordynowane podejście do identyfikowania, analizowania i usuwania podatności w całym cyklu życia programu.*

32 *UWAGA 3: Głównym celem jest utrzymanie wysokiego poziomu uzasadnienia zaufania w zakresie bezpieczeństwa poprzez ciągłe monitorowanie i przejrzystą komunikację pomiędzy Właścicielem programu, dostawcą portfela oraz właściwymi europejskimi organami nadzorczymi. Przebieg proceduralny, zilustrowany na Rysunek 2, określa odpowiedzialność za ocenę ryzyka, koordynację regulacyjną oraz obowiązkową wymianę informacji o podatnościach. Mechanizm ten zapewnia, że każda zidentyfikowana słabość techniczna jest niezwłocznie usuwana poprzez wewnętrzne działania naprawcze i aktualizacje po stronie dostawcy portfela, przy jednoczesnym umożliwieniu niezbędnego ujawnienia organom państw członkowskich oraz Europejskiej Bazie Danych o Podatnościach prowadzonej przez ENISA — chroniąc w ten sposób integralność i zaufanie do ekosystemu Portfela EUDI.*



Rysunek 2 Zarządzanie podatnościami technicznymi

33 *UWAGA 4: Właściciel programu jest informowany przez CAB-CB o podatnościach na podstawie raportu analizy wpływu (Impact Analysis Report) dostarczonego przez dostawcę portfela. Informacje przekazywane przez CAB-CB obejmują wszystkie elementy niezbędne Właścicielowi programu do zrozumienia wpływu podatności, zmian, jakie należy wprowadzić w jednym lub kilku elementach rozwiązania Portfela EUDI, oraz — o ile są dostępne — wszelkie informacje od CAB-CB dotyczące szerszych implikacji podatności dla innych certyfikowanych elementów rozwiązania Portfela EUDI. Szczegóły — zob. GP-02, GP-03.*

34 Po otrzymaniu informacji o podatności i przeanalizowaniu jej wpływu oraz wagi w odniesieniu do certyfikatu najwyższego poziomu, a także na podstawie decyzji CAB-CB o zawieszeniu certyfikatu najwyższego poziomu Właściciel systemu musi powiadomić Komisję Europejską o tym działaniu zgodnie z mechanizmem notyfikacji opisanym w pkt 7.1.2.

- 35 Dodatkowo Właściciel systemu musi udostępnić stosowne informacje o podatności Grupie ds. Współpracy na rzecz Portfela EUDI, ENISA (w razie potrzeby) oraz innym państwom członkowskim zgodnie z właściwymi uzgodnieniami wzajemnymi.
- 36 Właściciel programu musi monitorować status działań naprawczych. Do decyzji Właściciela programu należy przedłużenie okresu zawieszenia certyfikatu, jeżeli jest to uzasadnione.
- 37 Po zakończeniu sprawy Właściciel programu musi:
- o powiadomić Komisję Europejską o zmianie statusu certyfikatu najwyższego poziomu,
 - o poinformować odpowiednio wszystkich właściwych interesariuszy.
- 38 W przypadku gdy podatność dotyczy komponentu certyfikowanego w ramach programu EUCC, zastosowanie mają przepisy rozporządzenia wykonawczego Komisji 2024/482, rozdział VI „Zarządzanie podatnościami i ujawnianie podatności”. Właściciel programu musi współpracować z krajowym organem certyfikacji cyberbezpieczeństwa w celu obsługi podatności.

5 **Znaki i oznaczenia**

5.1 **Znak zaufania Portfela EUDI**

- 39 *UWAGA: Znak zaufania Portfela EU DI jest powiązany z certyfikatem najwyższego poziomu wydanym w ramach systemu certyfikacji PL Portfela EUDI zgodnie z procedurą określoną w GP-03.*
- 40 Zgodnie z rozporządzeniem (UE) 910/2014 oraz pkt 6.5.3.6 Ram Architektury i Odniesienia (ARF) użytkownikom należy zapewnić jednoznaczny sposób zweryfikowania, że instalują lub — po aktywacji — aktywnie używają zaufanego i certyfikowanego rozwiązania portfela.
- 41 Aby osiągnąć zgodność z tym wymaganiem regulacyjnym, instancja portfela certyfikowanego rozwiązania portfela musi zawierać dedykowany widok interfejsu użytkownika ze znakiem zaufania (Trust Mark UI). Gdy użytkownik wywoła znak zaufania w instancji portfela, interfejs — zgodnie ze specyfikacją — wykonuje następujące operacje:
- o Renderowanie grafiki: renderuje oficjalną grafikę i/lub logo znaku zaufania.

- o Wyświetlanie tekstu informacyjnego: wyświetla tekst informacyjny dotyczący certyfikacji rozwiązania portfela, który musi być zlokalizowany zgodnie z ustawieniami językowymi urządzenia użytkownika.
- o Link dotyczący certyfikacji: udostępnia link internetowy prowadzący bezpośrednio do listy certyfikowanych rozwiązań portfela oraz do konkretnej strony internetowej zawierającej informacje o certyfikacji aktywnego rozwiązania portfela użytkownika.

42 *UWAGA: Informacje dostępne poprzez łącza dotyczące certyfikacji są hostowane i dynamicznie zarządzane przez Komisję Europejską. Dokładna zawartość techniczna oraz konkretne procesy zasilania wymagane do renderowania tego widoku interfejsu na poziomie instancji portfela są zdefiniowane w Specyfikacji technicznej 1.*

43 Odniesienia:

- Rozporządzenie (EU) 910/2014
- ARF, pkt 6.5.3.6
- Specyfikacja techniczna 1: <https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts1-eudi-wallet-trust-mark.md> (dostęp: 21.06.2026)

5.2 **Znak zgodności w ramach Systemu Certyfikacji PL Portfela EUDI**

44 Właściciel systemu musi ustanowić oficjalny znak zgodności, który publicznie poświadcza pomyślne procesy oceny i certyfikacji odpowiedniego elementu rozwiązania portfela w ramach systemu certyfikacji PL Portfela EUDI.

45 Właściciel programu musi przyznać jednostkom oceniającym zgodność (CAB) akredytowanym przez polską jednostkę akredytującą w zakresie programów certyfikacji GP-01, GP-02 lub GP-03 prawo do używania znaku zgodności.

46 Jednostki oceniające zgodność – jednostki certyfikujące (CAB-CB) mają prawo do przenoszenia go na posiadaczy ważnych certyfikatów wydanych w ramach tych programów.

47 Właściciel systemu musi prowadzić rejestr podmiotów uprawnionych do
używania znaku zgodności, powiązanych certyfikatów oraz ich statusu
ważności (aktualny, zawieszony, cofnięty lub wygasły).

5.3 Projekt i formaty

48 Znak zgodności musi być prezentowany pod następującą marką:

49 „PL EUDI Wallet certification system” / „Polski system certyfikacji
Europejskiego Portfela Tożsamości Cyfrowej”.

50 *UWAGA: Prezentacja graficzna oraz zasady prezentacji wizualnej są
określone w dedykowanej publikacji Ministra Cyfryzacji.*

51 Logo musi być uzupełnione odpowiednim kodem QR zawierającym URL
strony lub portalu dostawcy portfela oraz dodatkowe informacje o
programie certyfikacji PL Portfela EUDI.

5.4 Zasady używania znaku zgodności

52 Znak zgodności może być używany wyłącznie w następujących
przypadkach:

- o wszelkie informacje związane z systemem certyfikacji PL Portfela EUDI wydawane i rozpowszechniane przez Właściciela systemu;
- o dokumentacja techniczna i handlowa certyfikowanego europejskiego portfela tożsamości wytwarzana przez posiadacza certyfikatu, w tym materiały informacyjne, specyfikacje produktów i prezentacje;
- o platformy informacyjne (strony internetowe, aplikacje, portale dedykowane usługom związanym z rozwiązaniem Portfela EUDI) powiązane z dostawcą certyfikowanego produktu lub usługi, pod warunkiem wyraźnego wskazania odpowiedniej certyfikacji;
- o oficjalne dokumenty wydawane przez CAB lub Właściciela programu, takie jak raporty publiczne, listy certyfikowanych produktów lub usług, dane statystyczne i inne materiały publiczne związane z przedmiotem.

53 Każde użycie znaku zgodności wykraczające poza katalog określony w pkt.
52 wymaga uprzedniej zgody Właściciela programu.

54 Używanie znaku zgodności jest zabronione w następujących przypadkach:

- o umieszczanie znaku zgodności na produktach, usługach lub wersjach, które nie są objęte wydanym certyfikatem;
- o modyfikowanie lub łączenie znaku zgodności ze znakami towarowymi lub innymi logotypami;
- o w powiązaniu z zawieszonym, cofniętym lub wygasłym certyfikatem wydanym w ramach systemu certyfikacji PL Portfela EUDI.

55

Każde niewłaściwe użycie znaku będzie przedmiotem działań prawnych podejmowanych przez CAB-CB, która przyznała prawo do używania znaku zgodności, na podstawie postanowień umownych pomiędzy CAB-CB a posiadaczem certyfikatu.

6 Ramy zaufania (Trust Framework)

6.1 Ramy regulacyjne nadzoru nad europejskim portfelem tożsamości cyfrowej

- 56 Organ nadzoru wyznaczony zgodnie z art. 46a ust. 1 rozporządzenia (UE) 910/2014 musi oficjalnie notyfikować Komisji Europejskiej swoje wyznaczenie wraz z wymaganymi danymi kontaktowymi.
- 57 Zgodnie z art. 46a ust. 3 rozporządzenia (UE) 910/2014 organ nadzoru musi zapewnić — zarówno poprzez działania nadzorcze ex ante, jak i ex post — że dostawcy i ich portfele stale spełniają wymagania regulacyjne, a także poprzez podejmowanie ukierunkowanych działań egzekucyjnych w przypadku uzyskania informacji o naruszeniach regulacyjnych.
- 58 Organ nadzoru musi wykonywać swoje zadania operacyjne, obejmujące:
- o współpracę transgraniczną z innymi organami nadzoru,
 - o żądanie od interesariuszy ekosystemu Portfela EUDI wszystkiego, co jest niezbędne do monitorowania zgodności,
 - o prowadzenie zarówno inspekcji na miejscu, jak i nadzoru zdalnego.
- 59 Organ nadzoru jest uprawniony do żądania od dostawców usunięcia wszelkich uchybień w zakresie zgodności oraz do zawieszenia lub anulowania rejestracji stron ufających w ramach wyznaczonego mechanizmu w przypadkach oszukańczego lub niezgodnego z prawem używania portfela.
- 60 Organ nadzoru musi koordynować z organem ochrony danych wszelkie działania dotyczące potencjalnych naruszeń przepisów lub naruszeń ochrony danych.
- 61 W zakresie reagowania na incydenty organ nadzoru musi zgłaszać istotne naruszenia bezpieczeństwa lub utraty integralności właściwym organom i pojedynczym punktom kontaktowym oraz informować opinię publiczną lub wymagać tego od dostawców, jeżeli takie ujawnienie służy interesowi publicznemu.
- 62 Zgodnie z art. 46a ust. 5 rozporządzenia (UE) 910/2014, jeżeli dostawca portfela nie zastosuje się do żądania naprawczego w terminie określonym przez organ, organ nadzoru jest uprawniony do nakazania zawieszenia lub całkowitego zaprzestania dostarczania europejskiego portfela tożsamości cyfrowej, z uwzględnieniem wagi, czasu trwania i skutków uchybienia.

Takie decyzje egzekucyjne muszą być przekazywane bez zbędnej zwłoki Komisji Europejskiej, organom nadzoru innych państw członkowskich, stronom ufającym oraz użytkownikom końcowym.

63 Zgodnie z art. 46a ust. 6 i art. 46a ust. 7 rozporządzenia (UE) 910/2014 organ nadzoru musi do 31 marca przekazać Komisji Europejskiej roczne sprawozdanie ze swoich głównych działań za poprzedni rok kalendarzowy.

64 *UWAGA: Sprawozdanie to jest następnie przekazywane Parlamentowi Europejskiemu i Radzie z wykorzystaniem znormalizowanych formatów i procedur administracyjnych ustanowionych przez Komisję w drodze aktów wykonawczych.*

6.2 Ramy zaufania: ustanowienie i utrzymanie pod egidą organu nadzoru

65 *UWAGA 1: Ekosystem Portfela EUDI opiera się na ustrukturyzowanych ramach aktorów nadzorujących i operacyjnych. Status tych aktorów jest formalizowany poprzez rejestrację i następującą po niej notyfikację Komisji Europejskiej.*

66 *UWAGA 2: Organ nadzoru nadzoruje funkcjonowanie dostawców portfela i innych uczestników ekosystemu, a ich wyznaczenie jest notyfikowane Komisji.*

67 *UWAGA 3: Architektura zaufania działa na dwóch odrębnych poziomach zarządzanych przez trzy główne role użytkowników. Państwa członkowskie tworzą i podpisują krajowe zaufane listy (TL), którymi zarządzają operatorzy TSL wraz z użytkownikami TSP utrzymującymi rekordy poszczególnych dostawców. Na poziomie europejskim Komisja Europejska wyznacza operatorów LoTL, którzy agregują te krajowe listy w jednolitą unijną listę zaufanych list (LoTL), czerpiącą swoje ostateczne źródło zaufania z Dziennika Urzędowego Unii Europejskiej.*

68 Aby ustanowić ramy zaufania w ekosystemie PL Portfela EUDI, organ nadzoru musi przypisać dedykowanym podmiotom: role wydawcy certyfikatów dostępu oraz wydawcy certyfikatów rejestracji.

69 Wydawcy ci muszą wydawać poświadczenia dostawcom PID, dostawcom QEAA, dostawcom PUB-EAA, dostawcom niekwalifikowanych EAA oraz stronom ufającym w celu zapewnienia autentyczności i ważności podczas interakcji z jednostkami portfela.

70 *UWAGA 4: Zgodnie z rozporządzeniem wykonawczym Komisji 2025/848 rola wydawcy certyfikatów dostępu i wydawcy certyfikatów rejestracji w odniesieniu do stron ufających jest przypisana dostawcom usług zaufania.*

71 *UWAGA 5: Certyfikaty rejestracji dla podmiotów publicznych mogą być wydawane przez Ministerstwo Cyfryzacji.*

72 Zgodnie z rozporządzeniem (UE) 2024/2980 organ nadzoru musi notyfikować tych wydawców Komisji Europejskiej z wykorzystaniem bezpiecznego elektronicznego systemu notyfikacji.

73 Po notyfikacji ich kotwice zaufania — obejmujące klucze publiczne i unikalne identyfikatory — muszą zostać opublikowane na zaufanej liście przez dostawcę zaufanej listy. Listy te są podpisywane i udostępniane poprzez prowadzoną przez Komisję listę zaufanych list, co umożliwia weryfikację poświadczeń w całym ekosystemie.

74 *UWAGA 6: Z technicznego punktu widzenia architektura, metadane, model podpisu kryptograficznego oraz format publikacji krajowych TL i unijnej LoTL ściśle i wyłącznie odpowiadają specyfikacji ETSI EN 119 612. Inne formaty, profile lub alternatywne podejścia do serializacji nie są na tym etapie obsługiwane, lecz zostaną włączone po oficjalnej publikacji normy ETSI EN 119 602.*

6.3 Zgodność dostawców portfela z ramami zaufania

75 Organ nadzoru musi informować Komisję Europejską o rejestracji i statusie dostawcy portfela oraz powiązanego z nim rozwiązania portfela.

76 Dostawca portfela musi zarejestrować siebie i swoje rozwiązanie portfela u wyznaczonego krajowego dostawcy zaufanej listy dostawców portfela.

77 *UWAGA 1: Minister Cyfryzacji wyznaczył Narodowy Bank Polski jako dostawcę zaufanej listy.*

78 Po pomyślnej rejestracji oraz zakończeniu odpowiednich procesów oceny i certyfikacji Właściciel systemu musi notyfikować dostawcę portfela Komisji Europejskiej.

79 Po zakończeniu tych procedur notyfikacyjnych kotwice zaufania dostawcy portfela muszą zostać ujęte na właściwej zaufanej liście dostawców portfela.

80 *UWAGA 2: Ta integracja umożliwia dostawcom PID i dostawcom poświadczeń weryfikację autentyczności poświadczeń jednostki portfela*

(WUA), potwierdzając, że wchodzi w interakcję z autentyczną jednostką portfela pochodzącą z zaufanego źródła.

81 *UWAGA 3: Komisja Europejska odpowiada za ustanowienie standardowych procedur operacyjnych wraz z systemem wymiany informacji, które umożliwiają zawieszanie lub anulowanie podmiotów uczestniczących w ekosystemie Portfela EUDI.*

82 Organ nadzoru musi zawiesić lub anulować zarejestrowanego dostawcę portfela po stwierdzeniu, że określone warunki regulacyjne nie są spełnione. W wyniku takich procedur status danego podmiotu na właściwej zaufanej liście musi zostać zmieniony na Invalid (nieważny). Następnie wszystkie ważne poświadczenia jednostki portfela (WUA) powiązane z jednostkami portfela wydanymi przez tego dostawcę muszą zostać unieważnione.

83 Odniesienia:

- ARF, Section 6.2.1
- ARF, Section 6.2.2

6.4 Sprawozdawczość dotycząca ekosystemu Portfela EUDI

6.4.1 Postanowienia ogólne

84 Zgodnie z art. 4 i załącznikiem II rozporządzenia (UE) 2024/2980 organ nadzoru musi przekazywać Komisji Europejskiej co najmniej szczegółowe informacje dotyczące każdej kategorii dostawców (w tym dostawców portfela, dostawców PID, dostawców QEAA oraz wydawców certyfikatów dostępu). Informacje te obejmują:

- oficjalne nazwy, numery rejestrowe (w stosownych przypadkach) oraz dane kontaktowe (e-mail/telefon);
- adresy URL właściwych polityk i warunków korzystania;
- co najmniej jeden certyfikat zgodny z RFC 3647, używany do uwierzytelniania i walidacji podpisów lub pieczęci podmiotu na dostarczanych przez niego danych.

85 *UWAGA: Komisja prowadzi i publikuje te listy zgodnie z art. 5 rozporządzenia (UE) 2024/2980, zapewniając ich dostępność bez rejestracji, z wykorzystaniem zaawansowanego szyfrowania warstwy transportowej oraz opatrzenie podpisami cyfrowymi lub pieczęciami. Wszelkie zmiany*

notyfikowanych informacji muszą być przekazywane Komisji bez zbędnej zwłoki, aby zapewnić dokładność publikowanych list.

86 Odniesienia:

87 Rozporządzenie (UE) 2024/2980: art. 4, art. 5, załącznik II.

88 ARF: pkt 3.13, 3.18, 3.19; 4.6.4, 6.3.2.1, 6.3.2.4.

6.4.2 Procedury notyfikowania Komisji Europejskiej ekosystemu Portfela EUDI

89 Zgodnie z art. 3 rozporządzenia wykonawczego Komisji (UE) 2024/2980 organ nadzoru musi informować Komisję Europejską o podmiotach i mechanizmach, o których mowa w art. 5a ust. 18 rozporządzenia (UE) nr 910/2014, tj.:

90 (a) organie odpowiedzialnym za ustanowienie i prowadzenie listy zarejestrowanych stron ufających korzystających z europejskich portfeli tożsamości cyfrowej zgodnie z art. 5b ust. 5 oraz o lokalizacji tej listy;

91 (b) organach odpowiedzialnych za dostarczanie europejskich portfeli tożsamości cyfrowej zgodnie z art. 5a ust. 1;

92 (c) organach odpowiedzialnych za zapewnienie, aby dane identyfikujące osobę były powiązane z europejskim portfelem tożsamości cyfrowej zgodnie z art. 5a ust. 5 lit. f);

93 (d) mechanizmie umożliwiającym walidację danych identyfikujących osobę, o których mowa w art. 5a ust. 5 lit. f), oraz tożsamości stron ufających;

94 (e) mechanizmie służącym do walidacji autentyczności i ważności europejskich portfeli tożsamości cyfrowej.

95 Wszystkie obowiązki sprawozdawcze organu nadzoru muszą być realizowane z wykorzystaniem systemu notyfikacji prowadzonego przez Komisję.

96 Dalsze szczegóły dotyczące konsekwencji zmian statusu zawiera pkt 6.2.3 ARF „Wallet Provider Suspension or Cancellation” (Zawieszenie lub anulowanie dostawcy portfela). Zgodnie z tym punktem państwo członkowskie może zdecydować o zawieszeniu lub anulowaniu dostawcy portfela. W takich przypadkach status dostawcy portfela na właściwej zaufanej liście musi zostać zmieniony na Invalid (nieważny). W konsekwencji dostawcy PID, dostawcy poświadczeń i strony ufające nie

mogą już ufać kotwicom zaufania tego dostawcy portfela i muszą w związku z tym odmawiać interakcji.

7 Szczególne procedury notyfikacji i sprawozdawczości w odniesieniu do systemu certyfikacji

7.1 Zmiany statusu certyfikatu

7.1.1 Notyfikacja wyników: procedury notyfikowania wyników certyfikacji i działań nadzoru Właścicielowi systemu/programu

97 Właściciel systemu musi utworzyć i prowadzić rejestr certyfikatów w oparciu o wymagania określone w rozporządzeniu (UE) 910/2014.

98 W celu realizacji notyfikacji i wyników działań nadzoru Właściciel systemu musi żądać od każdej CAB-CB informacji o certyfikatach wydanych, zawieszonych, wygasłych lub cofniętych w ciągu 48 godzin od zmiany danego statusu.

99 Właściciel systemu musi monitorować wszelkie zmiany statusu certyfikatów podrzędnych, które mają wpływ na status certyfikatu najwyższego poziomu.

100 W przypadku stwierdzenia, że jakikolwiek certyfikat, w tym certyfikat najwyższego poziomu, wygasł, został zawieszony lub cofnięty, Właściciel systemu musi odpowiednio zaktualizować rejestr certyfikatów.

7.1.2 Notyfikacja Komisji Europejskiej i EUDICG

101 *UWAGA: Zarządzanie cyklem życia rozwiązania portfela wymaga, aby Właściciel systemu notyfikował Komisji przejście rozwiązania portfela do stanu „Valid” (ważny, tj. certyfikowany). Ponadto w określonych warunkach regulacyjnych status certyfikatu podlegającego notyfikacji może ulec zmianie. Wywoła to działanie polegające na natychmiastowej aktualizacji rejestru certyfikatów i odpowiedniej notyfikacji Komisji w celu utrzymania integralności i wiarygodności ekosystemu Portfela EUDI.*

102 Właściciel systemu musi bez zbędnej zwłoki notyfikować Komisji i Grupie Współpracy certyfikację rozwiązania portfela (tj. certyfikat najwyższego poziomu), a także każde późniejsze wygaśnięcie, zawieszenie lub cofnięcie takiej certyfikacji.

103 W przypadku cofnięcia, Właściciel systemu musi podać przyczyny leżące u podstaw decyzji, aby zapewnić przejrzystość regulacyjną w całej Unii.

104 Właściciel systemu musi przekazywać notyfikacje sporządzone co najmniej w języku angielskim za pośrednictwem bezpiecznego elektronicznego systemu notyfikacji. Komisja jest uprawniona do żądania dodatkowych informacji lub wyjaśnień w celu zweryfikowania kompletności i spójności notyfikowanych danych.

105 Odniesienia:

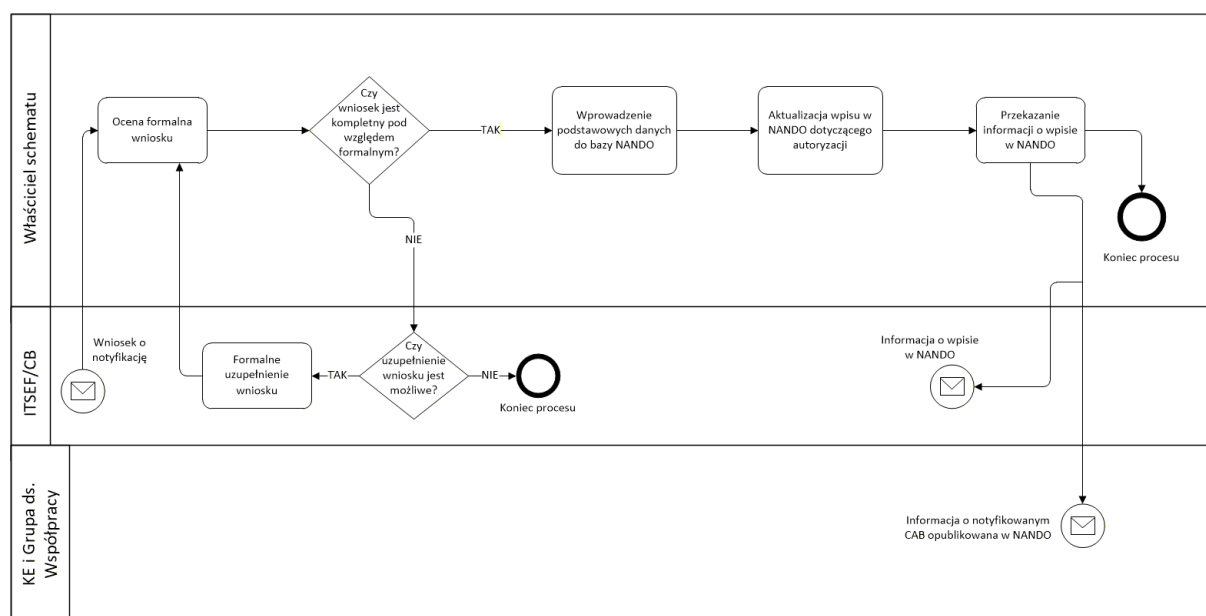
- Rozporządzenie (UE) 2024/2980, art. 4 ust. 1, 2 i 3
- Rozporządzenie (UE) 910/2014, art. 5d
- ARF, Section 6.2.1
- ARF, Section 6.2.2

7.2 Notyfikacja w NANDO

106 *UWAGA: Niniejszy punkt opisuje procedurę, dlatego stosuje proste stwierdzenia faktów.*

7.2.1 Pierwsza notyfikacja polskich CAB w NANDO

107 Proces pierwszej notyfikacji polskiej jednostki oceniającej zgodność (CAB) do bazy danych NANDO jest kluczową procedurą administracyjną, która formalizuje uprawnienie CAB do prowadzenia działań certyfikacyjnych w ekosystemie Portfela EUDI.

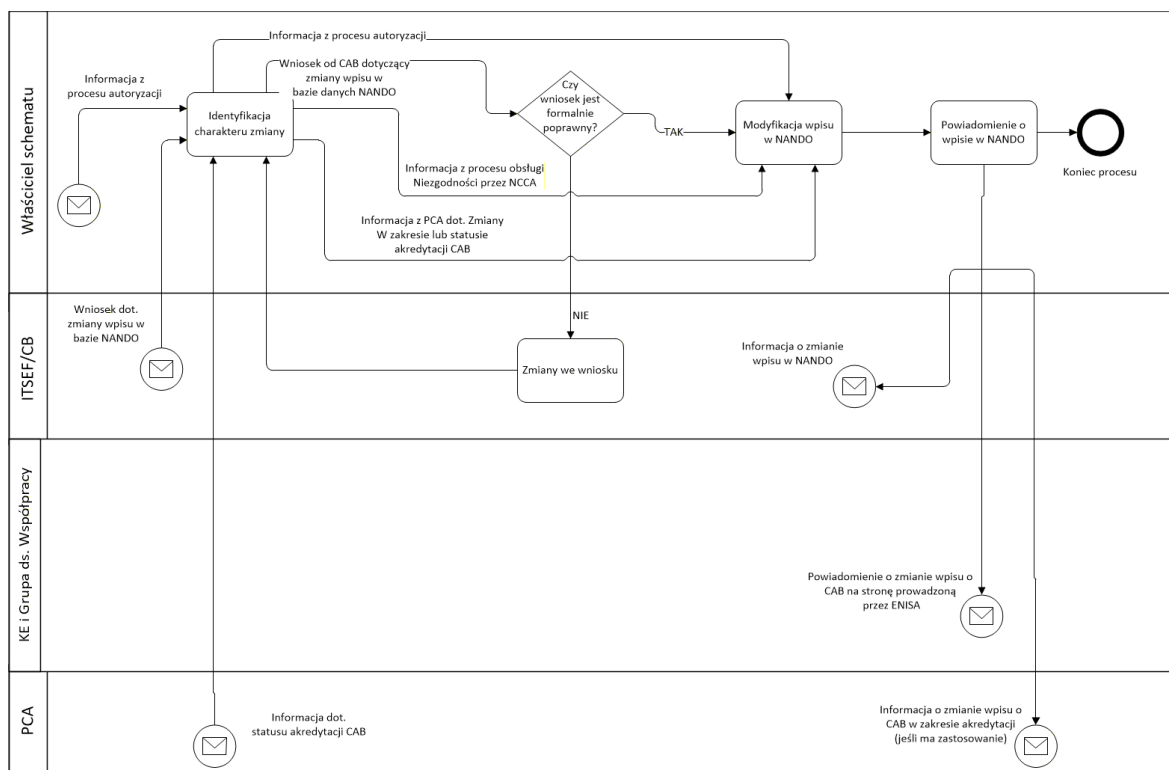


Rysunek 3 Notyfikacja polskich CAB — pierwszy wpis w NANDO

- 108 Przebieg rozpoczyna się od złożenia przez CAB-ITSEF/CB formalnego wniosku o notyfikację do Właściciela programu.
- 109 Po jego otrzymaniu Właściciel programu przeprowadza przegląd formalny w celu weryfikacji kompletności i zgodności regulacyjnej wniosku. W przypadku stwierdzenia braków CAB-ITSEF/CB jest zobowiązana do dostarczenia niezbędnych uzupełnień; w przeciwnym razie proces zostaje zakończony. Po zweryfikowaniu formalnej kompletności wniosku Właściciel programu wprowadza podstawowe dane do systemu NANDO i dokonuje niezbędnych aktualizacji dotyczących zakresu uprawnień CAB.
- 110 Po aktualizacji wpisu w NANDO Właściciel programu przekazuje CAB-ITSEF/CB oficjalne potwierdzenie. Ponadto, zgodnie z wymaganiami przejrzystości rozporządzenia (UE) 910/2014, Właściciel programu formalnie notyfikuje Komisji Europejskiej oraz Grupie Współpracy nowo uprawnioną CAB, zapewniając publikację wpisu w NANDO oraz oficjalne uznanie CAB w zakresie krajowego systemu certyfikacji w Państwie Członkowskim.

7.2.2 Aktualizacje wpisów w NANDO

- 111 Proces aktualizacji wpisów w NANDO zapewnia, że publikowane informacje dotyczące jednostki oceniającej zgodność (CAB) pozostają dokładne i odzwierciedlają jej aktualny status operacyjny oraz zakres akredytacji.



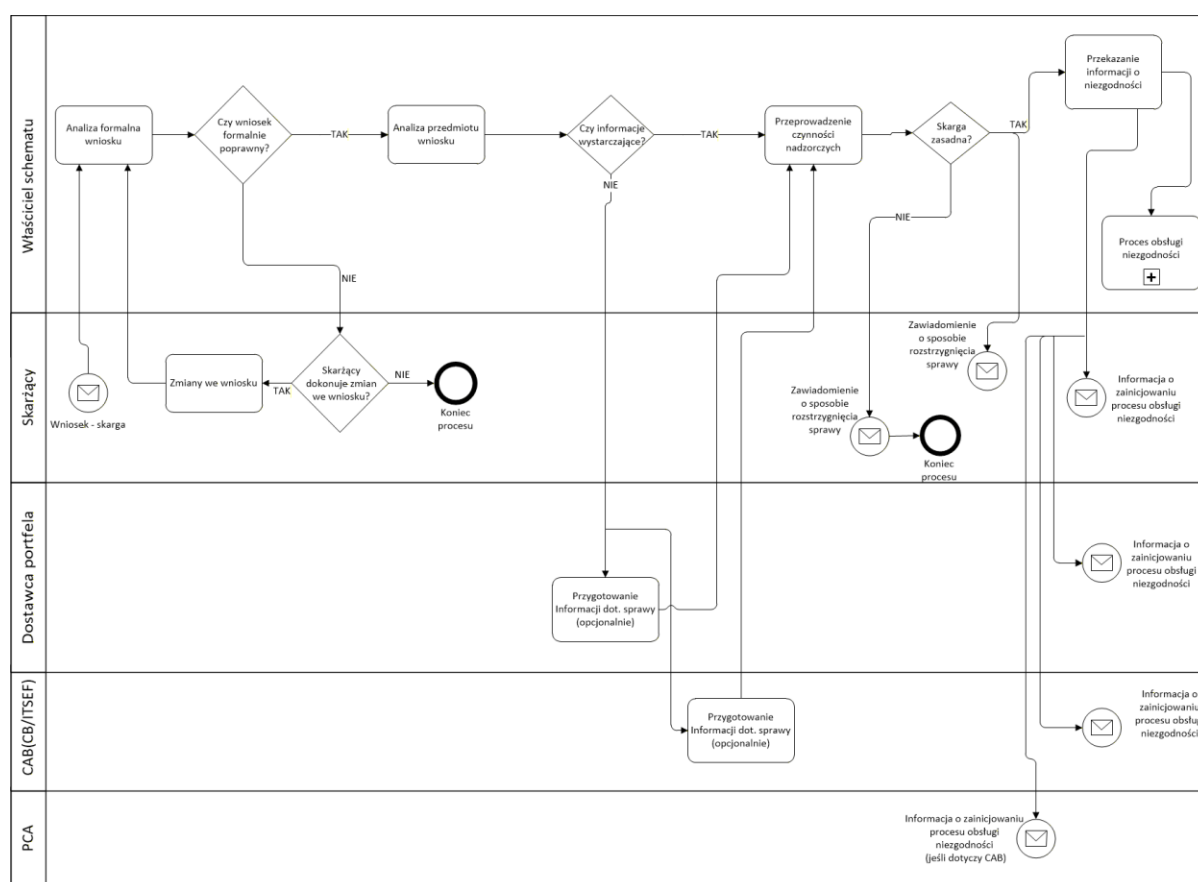
Rysunek 4 Notyfikacja polskich CAB — zmiana wpisu w NANDO

- 112 Przebieg jest uruchamiany albo formalnym wnioskiem o zmianę wpisu złożonym przez CAB-TSEF/CB, albo automatycznie po otrzymaniu informacji z Polskiego Centrum Akredytacji (PCA) o zmianie zakresu lub statusu akredytacji CAB.
- 113 Po otrzymaniu bwyzwalacza Właściciel programu identyfikuje charakter zmiany i poddaje wniosek formalnej weryfikacji poprawności. W przypadku stwierdzenia braków CAB-ITSEF/CB jest zobowiązana do dostarczenia niezbędnych poprawek; w przeciwnym razie proces zostaje zakończony.
- 114 Po zweryfikowaniu wniosku Właściciel programu dokonuje modyfikacji wpisu w systemie NANDO. Właściciel programu formalnie notyfikuje Komisji Europejskiej i Grupie ds. Współpracy zaktualizowany wpis. Zapewnia to, że baza danych NANDO pozostaje wiarygodnym, aktualnym źródłem uprawnionych CAB, chroniąc integralność ram certyfikacji Portfela EUDI.

8 Rozpatrywanie skarg

115 UWAGA: W niniejszym rozdziale opisano procedurę, dlatego zastosowano proste stwierdzenia faktów

116 Proces rozpatrywania skarg stanowi ustrukturyzowany mechanizm umożliwiający Właścicielowi programu utrzymanie skutecznego nadzoru i zapewnienie rozliczalności programu Portfela EUDI. Procedura ta ułatwia formalne przyjmowanie, bezstronne badanie i rozstrzyganie skarg, zapewniając systematyczne rozpatrywanie wszystkich kwestii zgłaszanych przez interesariuszy.



Rysunek 5 Rozpatrywanie skarg

117 Procedura rozpoczyna się od formalnej analizy przeprowadzanej przez Właściciela programu po otrzymaniu skargi. Jeżeli zgłoszenie zawiera braki formalne, Właściciel programu nawiązuje kontakt ze skarżącym w celu zażądania niezbędnych uzupełnień lub wyjaśnień. Po skompletowaniu wniosku Właściciel programu przeprowadza wnikliwą analizę merytoryczną w celu ustalenia zakresu i zasadności skargi.

- 118 W fazie wyjaśniającej Właściciel programu pełni rolę centralnego koordynatora. W zależności od przedmiotu sprawy Właściciel programu może formalnie zażądać od dostawcy Portfela EUDI przedłożenia dowodów lub stanowisk technicznych związanych ze sprawą. W przypadkach obejmujących złożone zagadnienia techniczne Właściciel programu może również zlecić jednostce oceniającej zgodność dostarczenie dokumentacji eksperckiej lub opinii dotyczącej zgodności portfela. Jeżeli wstępne informacje okażą się niewystarczające do stwierdzenia potencjalnej niezgodności, Właściciel programu zastrzega sobie prawo do zlecenia dedykowanych działań nadzorczych lub skorzystania ze wsparcia zewnętrznych niezależnych ekspertów na każdym etapie procesu.
- 119 Ostatni etap procedury obejmuje formalne rozstrzygnięcie i przekazanie ustaleń. Jeżeli skarga zostanie uznana za bezzasadną, Właściciel programu wydaje skarżącemu zawiadomienie zawierające uzasadnienie rozstrzygnięcia. Jeżeli skarga zostanie uznana za zasadną, Właściciel programu zawiadamia skarżącego, a w stosownych przypadkach przekazuje odpowiednie informacje dostawcy Portfela EUDI i jednostce oceniającej zgodność. Ponadto w przypadku potwierdzonej niezgodności Właściciel programu formalnie zawiadamia skarżącego, jednostkę oceniającą zgodność, dostawcę Portfela EUDI oraz krajową jednostkę akredytującą o wszczęciu procesu dotyczącego niezgodności. Zapewnia to pełną identyfikowalność i przestrzeganie wymagań nadzoru certyfikacyjnego, chroniąc integralność i wiarygodność krajowych ram tożsamości.
- 120 W przypadku gdy skarga zostanie wniesiona zgodnie z art. 25 ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa, Właściciel programu musi współpracować z krajowym organem certyfikacji cyberbezpieczeństwa i przekazać mu informacje niezbędne do oceny skargi.

9 Procedury techniczne Właściciela systemu

9.1 Ochrona informacji

121 *UWAGA: W trakcie procesów oceny i certyfikacji jednostki oceniające zgodność oraz Właściciel programu pozyskują dane poufne i wrażliwe oraz tajemnice przedsiębiorstwa, także odnoszące się do własności intelektualnej lub monitorowania zgodności, które wymagają odpowiedniej ochrony.*

122 Właściciel programu/systemu, EUDICG, Komisja Europejska, jednostki CAB oraz wszyscy pozostali interesariusze muszą zapewnić bezpieczeństwo i ochronę tajemnic handlowych oraz innych informacji poufnych, w tym tajemnic przedsiębiorstwa, a także zachowanie praw własności intelektualnej.

123 Wszystkie zainteresowane strony muszą wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony informacji.

9.2 Bezpieczna wymiana informacji

9.2.1 Najnowocześniejsze mechanizmy kryptograficzne zatwierdzone przez Właściciela systemu

124 Właściciel systemu musi wyznaczyć i przyjąć mechanizmy kryptograficzne określone we właściwych specyfikacjach technicznych Ram Architektury i Odniesienia (ARF), w ścisłej zgodności z wymaganiami bezpieczeństwa określonymi w załączniku I rozporządzenia wykonawczego Komisji (UE) 2024/2979. Mechanizmy te są wymagane w celu zapewnienia bezpieczeństwa, integralności i poufności danych wymienianych w ekosystemie Portfela EUDI, zgodnie ze wspólnymi unijnymi standardami kryptograficznymi wymaganymi dla interoperacyjności transgranicznej.

125 Odniesienie: ARF (Specyfikacje techniczne), rozporządzenie (UE) 2024/2979, załącznik I.

9.2.2 Lista stosowanych mechanizmów i aplikacji dla CAB-CB, CAB-ITSEF i wnioskodawców

126 Właściciel systemu musi prowadzić i rozpowszechniać wykaz stosowanych mechanizmów kryptograficznych i aplikacji technicznych przeznaczonych do użytku przez jednostki oceniające zgodność (CAB) oraz wnioskodawców.

127 *UWAGA: Lista zatwierdzonych mechanizmów i aplikacji może być zawarta w dedykowanej publikacji Ministra Cyfryzacji.*

